REMARKS

Claims 1-43 are pending in the application. As a preliminary matter, Applicant would like to thank the Examiner for the courtesy of an interview with Applicant's representative. Claims 1-43 have been rejected. Claims 1, 6, 11, 15-16, 34, 37-38 and 41-42 have been currently amended. Claims 4, 5, 17-33 and 36 have been cancelled. Claims 44-55 have been added. No new matter is introduced herein. In view of the following remarks, reconsideration and withdrawal of these grounds for rejection is requested.

Claim Rejections Under 35 U.S.C. §101

Claim 17 stands rejected under 35 U.S.C. §101 as being directed toward non-statutory subject matter. Claim 17 has been canceled. As such, this rejection has been rendered moot.

Claim Rejections Under 35 U.S.C. §102

Claims 1-3, 5, and 17-19 stand rejected under 35 U.S.C. §102(b) as being anticipated by Ono (U.S. 2002/0035685 A1). Claims 4, 17-19 have been canceled. Independent Claim 1 has been amended. Claim 1 now reads:

A system for processing of information over a network comprising:

> at least first and second -processing devices and an interface, the first processing device for transmitting a communication having a desired destination being the second processing device, the first processing device also transmitting the security information associated with the communication, wherein said security information includes biometric information of the originator for identifying the originator of the communication, the communication and security information being received by the interface, the interface having access for processing a subset of the security information and communication to identify an

authorized condition, with the interface processing the subset of security information and communication by comparing the security information against previously stored security information to determine when there is a match between the security information and stored security information indicating an authorized condition, the interface transmitting the communication to the second processing device on identification of an authorized condition, the communication being retained at the interface or transmitted to a third secured processor on identification of an unauthorized condition, where there is no match made between the security information and stored security information, so that the communication does not reach the second processing device, the system further comprising a storage device containing the security information in electronic form that is communicated to the first processing device, wherein the storage device comprises a smart card. (Emphasis Added)

Therefore Claim 1 now requires that the security information is stored on a smart card and includes biometric information for identifying the originator of the communication. Further, the interface has access to only a subset of the security information and communication to identify an authorized condition, wherein the authorized condition is indicated by a match between the security information and stored security information. In the event of an unauthorized condition, the communication is retained at the interface or transmitted to a secure processor. As such, the system in amended Claim 1 is operable to secure against data communications from unauthorized users as well as to ensure the privacy of data communications of authorized users.

Ono relates to an intermediary device that is provided between a server and a client that has a management table for storing security information for at least one of server/client authentication, encryption/decryption and session information regarding a session between the server and the client. However, Ono does not disclose using biometric information for authentication, as the invention is directed toward the authentication of the devices employed for

data communication rather than the users of such devices. Further, Ono does not disclose an authentication means which is limited to accessing only a subset of information from a data communication for determining an authorized or unauthorized condition, wherein the intermediary device does not have access to the remaining portions of the data communication. Ono also does not disclose transmitting a communication to a secure processor in the event of an unauthorized condition. As such, because Ono does not disclose such features, Ono cannot anticipate Claim 1 as amended. In addition, Claims 2-3 and 6 depend from amended claim 1 and, as such, cannot be anticipated by Ono for the reasons cited in reference to Claim 1 above.

Claims 34-38 and 43 stand rejected under 35 U.S.C. §102(b) as being anticipated by Lofgren (U.S. 2001/0037313 A1). Claim 36 has been canceled. Independent Claim 34 has been amended. Claim 34 now reads:

A method of information processing comprising:
storing identifying information on a card, wherein said identifying information comprises biometric information including fingerprint information for identifying an owner of the card;
reading the stored identifying information from said card;
creating an authentication mark based at least in part on the read identifying information;
transmitting information along with the authentication mark-;
receiving the information along with the authentication mark at a first destination;
verifying whether the information is authorized based on the authentication mark and a subset of the information; and transmitting authorized information to a second destination. (Emphasis Added)

Therefore, Claim 34 now requires the identifying information to include biometric information for identifying a user. Further, Claim 34 requires the verification of whether the information is authorized to be based on the authentication mark and a subset of the information.

As such, other portions of the information cannot be accessed for the purposes of authorization.

Lofgren relates to systems which are responsive to watermarked documents to facilitate various transactions such as secure online transactions. The central site includes a database of image hashes and is in communication with a user terminal which may communicate a watermarked document. A watermark reader reads the watermark, computes a hash of the captured image and passes the hash to the central site for comparison with the images in the database.

However, Lofgren does not disclose a watermark reader or central site that has access only to a subset of the data contained in the watermarked document for determining authorization. While Lofgren does disclose a pin code, this code is utilized for verifying the identity of the user attempting to transmit data rather than for restricting access to subsets of the data communication from other elements of the system. See Lofgren, para. 0069. As such, in contrast to amended Claim 34, the security of the contents of the watermarked document in Lofgren is not ensured during the transmission between terminals by the use of a pin code. Therefore, because Lofgren does not disclose such features, Lofgren cannot anticipate Claim 34 as amended. Claims 35, 37-38 and 43 depend from amended Claim 34 and, as such, cannot be anticipated by Lofgren for the reasons cited in reference to Claim 34 above.

Claim Rejections Under 35 U.S.C. §103

Claims 4, 6-16, 20-33, 39-42 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Ono (U.S. 2002/0035685 A1) in view of Lofgren (U.S. 2001/0037313 A1).

The Examiner correctly points out that Ono does not disclose or suggest the stored security information comprising biometric information. Further, neither Lofgren nor Ono discloses or suggests the limitations of claim 1 as amended, namely, an authentication means (e.g., an interface) which is limited to accessing only a subset of information from a data communication for determining an authorized or unauthorized condition, wherein the authentication means does not have access to subsets of the data communication. Further, neither Lofgren or Ono discloses or suggests transmitting a communication to a secured processor, when there is no match made between the security information from the communication and the stored security information. Therefore, even if, arguendo, Lofgren is combinable with Ono, the combination of Lofgren and Ono does not disclose or suggest both securing a target processor against data communications from unauthorized users and ensuring the privacy of data communications of authorized users.

As to claims 10, 24(now canceled) and 40 (the office action inadvertently identifies 41), it is indicated in the office action that "it is well known in the art to use the GPS tracking device or IP address on the card", and "[o]ne of ordinary skill in the art would have been motivated to use GPS tracking device on the card for providing location information." This rejection is respectfully traversed. In particular, there is no art of record that either teaches, discloses or suggests the use of a GPS tracking device on the card, reader or computer, or the IP address of the computer, in combination with a system, computer readable medium or method as claimed by applicant, in order to provide location information. The only cited references, Ono and Lofgren, are silent as to each of these aspects.

The ability to identify and later track the originator of a transmission, as per Applicant's claims 10 and 40, is an important aspect for security. It provides a recipient with a mechanism to identify from where a transmission originated, in order to assess if it came from a reliable source or not. Also, it provides a mechanism by which an originator of any improper or illegal communications, such as hackers or a sender of any viruses or worms, can later be identified, and if necessary, apprehended. The ability to identify the originator also serves as a deterrent to would be offenders, since their identity would be easily discovered.

In view of the forgoing, applicant respectfully solicits that the rejection of claims 10 and 40 be withdrawn, or if the rejections are not withdrawn, that specific prior art be cited in order to support maintaining of the current rejections.

Claims 4 and 20-33 have been canceled. Claims 6-16 now depend, either directly or indirectly, from amended Claim 1 and Claims 39-42 depend either directly or indirectly from

amended Claim 34, which has been amended similarly to Claim 1. As such, Claims 6-16 and 39-42 cannot be rendered unpatentable by Ono in view of Lofgren.

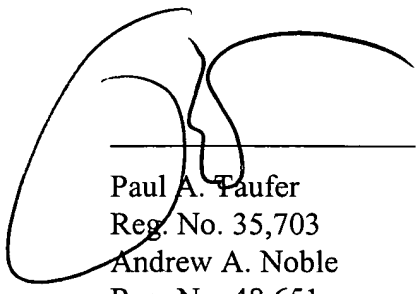
Claims 44-55 have been newly added for consideration. Independent Claim 44 is directed toward a computer-readable medium having computer-executable instructions for performing steps comprising receiving a data communication comprising biometric information for a user at a device for storing said data; comparing a subset of said data communication with locally stored information; and enabling the further transmission of said data communication when a match is found between said received data communication and said locally stored information.

Therefore, no new matter is introduced herein and favorable consideration of these claims is requested.

Conclusion

In view of the foregoing remarks, the Applicants submit that the Application is now in condition for allowance, which action is earnestly solicited.

Respectfully submitted,



Paul A. Taufer
Reg. No. 35,703
Andrew A. Noble
Reg. No. 48,651

PAT:nn
(215) 656-3385